

New Symmetric and Asymmetric Quantum Codes

Kenza Guenda and T. Aaron Gulliver *

Abstract

The asymmetric CSS construction is extended to the Hermitian case. New infinite families of quantum symmetric and asymmetric codes are constructed. The codes obtained are shown to have parameters better than those of previous codes. A number of known codes are special cases of the codes given here.

1 Introduction

Quantum codes have been introduced as an alternative to classical codes for use in quantum communication channels. Since the landmark result in [21] and [23], this field of research has grown rapidly. In particular, classical codes have been used to construct good quantum codes [5]. Until recently, most of the codes have been designed under the assumption that the channel is symmetric. Ioffe and Mézard [17] argued that in physical systems the noise is typically asymmetric, i.e., qubit-flip errors occur less frequently than phase-shift errors, so to design efficient error correcting codes, this asymmetry should be exploited. Using this fact, Ioffe and Mézard obtained asymmetric quantum error correcting codes from BCH and LDPC codes. They showed that these codes have good performance.

The Calderbank-Shor-Steane (CSS) construction uses a pair of classical codes, one for correcting qubit-flip errors and the other for correcting phase-shift errors [6,24]. The concept of asymmetric codes was introduced by Steane [25]. Sarvepalli et al. [19] extended the CSS construction to asymmetric stabilizer codes. The classical codes were chosen such that the code for phase errors has a larger distance than the code for qubit-flip errors. Further, they showed the advantage of asymmetric quantum codes over symmetric quantum codes, and gave several infinite families of asymmetric quantum codes obtained from nested classical codes. A mathematical framework for asymmetric quantum codes and some construction results were given in [27]. This framework was extended to additive codes by Ezerman et al. [12,13].

*T. Aaron Gulliver is with the Department of Electrical and Computer Engineering, University of Victoria, PO Box 3055, STN CSC, Victoria, BC, Canada V8W 3P6. email: agullive@ece.uvic.ca.

In this paper, we extend the asymmetric CSS construction to the Hermitian case. New infinite families of quantum codes are presented. In addition, new symmetric and asymmetric quantum codes are obtained from binary BCH codes. These codes have known minimum distances, and the relationship between the rate gain and minimum distance is given explicitly. The minimum distances are larger than those of the codes given in [1]. The concatenation of MDS codes is used to obtain new quantum codes. These codes have good parameters and provide significantly more flexibility in code design than the construction of Ezerman et al. [13].

2 Preliminaries

For a positive integer n , let $V_n = (\mathbb{C}^q)^{\otimes n} = \mathbb{C}^{q^n}$, be the n th tensor product of \mathbb{C}^q . Then V_n has the following orthonormal basis $\{|c\rangle = |c_1, \dots, c_n\rangle, c = (c_1, \dots, c_n) \in \mathbb{F}_q^n\}$. A q -ary quantum code of length n is a subspace Q of V_n of dimension k .

Definition 2.1 *Let d_x and d_z be positive integers. A quantum code Q in V_n with $K \geq 1$ codewords is called an asymmetric quantum code (AQC) with parameters $((n, K, \{d_z, d_x\}))_q$ or $[[n, k, \{d_z, d_x\}]]_q$ (with $k = \log_q K$), if Q detects $d_x - 1$ quantum symbols of x errors and also $d_z - 1$ quantum symbols of z errors.*

Lemma 2.2 *(Standard CSS Construction for AQCs)*

(i) *Let \mathcal{C}_1 and \mathcal{C}_2 be two classical codes over \mathbb{F}_q with parameters $[n, k_1, d_1]$ and $[n, k_2, d_2]$, respectively, such that $\mathcal{C}_1 \subset \mathcal{C}_2 \subset \mathbb{F}_q^n$. Then there exists a quantum code with parameters $[[n, k_2 - k_1, \{d_z, d_x\}]]_q$, where $d_z = \max\{wt(\mathcal{C}_2 \setminus \mathcal{C}_1), wt(\mathcal{C}_1^\perp \setminus \mathcal{C}_2^\perp)\}$ and $d_x = \min\{wt(\mathcal{C}_2 \setminus \mathcal{C}_1), wt(\mathcal{C}_1^\perp \setminus \mathcal{C}_2^\perp)\}$.*

(ii) *If there exists two classical linear codes \mathcal{C}_1 and \mathcal{C}_2 over \mathbb{F}_{q^2} with parameters $[n, k_1, d_1]_{q^2}$ and $[n, k_2, d_2]_{q^2}$ such that $\mathcal{C}_1^{\perp h} \subset \mathcal{C}_2$, then there exists an asymmetric quantum code with parameters $[[n, k_2 - k_1^h, \{d_x, d_z\}]]_{q^2}$, where $\{d_x, d_z\} = \{d_1, d_2\}$.*

Proof. Part (i) follows from the restatement of the CSS construction for asymmetric stabilizer codes given in [19, Lemma 3.1]. For (ii), we have that if a code is \mathbb{F}_{q^2} -linear then the Hermitian dual is the same as the trace Hermitian dual [5, Theorem 3]. Hence from [12, Theorem 4.5], there exists an asymmetric code with parameters $[[n, k_2 - k_1^h, \{d_z, d_x\}]]_{q^2}$, where $\{d_z, d_x\} = \{d_1, d_2\}$. \square

Note that an asymmetric quantum code with parameters $((n, K, \{d, d\}))_q$ is a symmetric quantum code with parameters $((n, K, d))_q$, but the converse is not true [27, Remark 2.3]. An AQC is pure whenever $\{d_z, d_x\} = \{d_1, d_2\}$, otherwise it is said to be degenerate.

A negacyclic code C of length n over \mathbb{F}_q such that $(n, q) = 1$ is an ideal of the ring $R = \mathbb{F}_q[x]/(x^n + 1)$, generated by a polynomial $g(x)$ which divides $x^n + 1$. The code C is

uniquely determined by its defining set $T = \{0 \leq i \leq 1 \mid g(\alpha^i) = 0\}$, where α is a $2n$ th primitive root of the unity. The following lemma characterizes the defining set of these codes.

Lemma 2.3 (*[14, Lemma 13]*) *Let O_n be the set of odd integers from 1 to $2n - 1$. If C is negacyclic over \mathbb{F}_{q^2} , then the Hermitian dual $C^{\perp h}$ is also negacyclic with defining set $\{i \in O_n : i \notin -qT\}$.*

Lemma 2.4 (*[9, Theorem 6.1]*) *Let C be a linear $[n, k, d]_q$ code. If C contains the all one codeword, then there exists an asymmetric quantum code Q with parameters $[[n, k - 1, \{d, 2\}]]_q$.*

Using Lemma 2.4, Chee et al. [9, Corollary 6.2] constructed some asymmetric quantum maximum distance separable (AQMDS) codes. This lemma can be used to obtain many AQCs (not necessarily MDS), as shown in the following.

Theorem 2.5 *There exist asymmetric quantum codes with the following parameters:*

- (i) $[[n, k - 1, \{d, 2\}]]_q$, and $[[n - 1, k - 1, \{d - 1, 2\}]]_q$ with n, k, d the parameters of a q -ary narrow-sense BCH code.
- (ii) $[[n, n/2 - 1, \{d, 2\}]]_2$, with n, d the parameters of any binary self-dual code.
- (iii) $[[2^m - 1, m, \{2^{m-1} - 1, 2\}]]_2$.

Proof. For part (i), a narrow-sense classical BCH code of designed distance δ over \mathbb{F}_q is a cyclic code generated by $g(x) = \text{lcm}(M_1, \dots, M_{\delta-1})$ that contains the all one codeword. Hence from Lemma 2.4, there is a quantum asymmetric code with parameters $[[n, k - 1, \{d, 2\}]]_q$. By puncturing a narrow-sense BCH code, we obtain a linear code which also contains the all one codeword. The dimension is k . Since a BCH code is cyclic, its permutation group is transitive. Hence the minimum distance has been decreased by one [26, Corollary 15 Ch. 8]. For part (ii), it is well known that the dual of a binary self-orthogonal code contains the all one codeword, hence the result follows from Lemma 2.4. For part (iii), the simplex code S_m is a code with parameters $[2^m - 1, m, 2^{m-1}]_2$. It is a cyclic code generated by $x^n - 1/M_1^*(x)$, where $M_1^*(x)$ is the reciprocal polynomial associated with $Cl(1)$, the cyclotomic class of 1. This is a subcode of the cyclic code \mathcal{C}_0 generated by $f_1(x) = x^n - 1/(x - 1)M_1^*(x)$. \mathcal{C}_0 is a $[2^m - 1, m + 1, 2^{m-1} - 1]$ code. The codeword $f_1(x)M_1^*(x)$ is equal to the all one codeword and is in \mathcal{C}_0 . Hence there exists an asymmetric quantum code with parameters $[[2^m - 1, m, \{2^{m-1} - 1, 2\}]]_2$. \square

Table 1: $[[15, k', \{d_z, 2\}]]_4$ codes obtained from BCH codes over \mathbb{F}_4 .

k'	2	3	5	7	8	10
d_z	11	10	7	6	5	3

Table 2: $[[n, k, \{d_x, d_z\}]]_4$ Asymmetric quantum codes obtained from punctured BCH codes over \mathbb{F}_4 .

$[[14, 6, \{6, 2\}]]_4$	$[[20, 9, \{6, 2\}]]_4$	$[[32, 8, \{10, 2\}]]_4$
$[[14, 9, \{4, 2\}]]_4$	$[[20, 12, \{4, 2\}]]_4$	$[[32, 18, \{7, 2\}]]_4$
$[[30, 21, \{4, 2\}]]_4$	$[[30, 16, \{6, 2\}]]_4$	$[[30, 11, \{10, 2\}]]_4$
$[[34, 8, \{6, 2\}]]_4$	$[[34, 17, \{4, 2\}]]_4$	$[[34, 23, \{2, 2\}]]_4$
$[[38, 27, \{2, 2\}]]_4$	$[[38, 21, \{8, 2\}]]_4$	$[[38, 15, \{9, 2\}]]_4$
$[[38, 9, \{12, 2\}]]_4$	$[[40, 11, \{19, 2\}]]_4$	$[[40, 21, \{8, 2\}]]_4$
$[[44, 31, \{4, 2\}]]_4$	$[[44, 26, \{6, 2\}]]_4$	$[[44, 20, \{8, 2\}]]_4$
$[[44, 15, \{10, 2\}]]_4$	$[[44, 9, \{12, 2\}]]_4$	$[[50, 27, \{8, 2\}]]_4$
$[[50, 23, \{13, 2\}]]_4$	$[[50, 19, \{16, 2\}]]_4$	$[[62, 39, \{10, 2\}]]_4$
$[[62, 27, \{20, 2\}]]_4$	$[[62, 11, \{30, 2\}]]_4$	$[[62, 8, \{41, 2\}]]_4$
$[[64, 9, \{38, 2\}]]_4$	$[[64, 11, \{12, 2\}]]_4$	$[[64, 17, \{12, 2\}]]_4$
$[[64, 29, \{12, 2\}]]_4$	$[[64, 35, \{10, 2\}]]_4$	$[[64, 47, \{5, 2\}]]_4$

Table 3: Quantum Code Comparison

New asymmetric codes	Asymmetric codes in [1]
$[[1023, 803, \{31, 15\}]_2$	$[[1023, 80, \{32, 15\}]_2$
$[[1023, 823, \{31, 11\}]_2$	$[[1023, 100, \{32, 11\}]_2$
$[[1023, 843, \{31, 7\}]_2$	$[[1023, 120, \{32, 7\}]_2$
$[[1023, 863, \{31, 3\}]_2$	$[[1023, 140, \{32, 3\}]_2$

Example 2.6 Applying (i) in Theorem 2.5, we obtain the $[[15, k', \{d_z, 2\}]_4$ codes listed in Table 1 from the $[15, k, d]_4$ BCH codes. Note that these codes have parameters similar to those in [13, Table 1] obtained via the best known linear codes (BKLCs). For example, we have the existence of codes with parameters $[[64, 29, \{12, 2\}]_4$ and $[[64, 9, \{38, 2\}]_4$. Note that in [13, Table 2], codes with parameters $[[64, 29, \{\geq 4, 2\}]_4$ and $[[64, 9, \{\geq 24, 2\}]_4$ were obtained using the concatenated RS code construction.

2.1 Quantum BCH Codes

The idea of constructing CSS codes from BCH codes is not new, as Steane [22] and Aly et al. [1, 2] give quantum symmetric and asymmetric codes. The difficulty with their methods is the lack of knowledge of the dual distances, as noted in [19]. In addition, there is a rate gain which is linearly proportional to the reduction in the distance of the code used for correcting qubit-flip errors [19, Lemma 4.6]. Here we give quantum BCH codes with known minimum distances that have a rate gain larger than the codes in [19, Lemma 4.6].

Lemma 2.7 Let $n = 2^m - 1$ and $B(\delta_i)$ be the BCH code of designed distance δ_i such that $2 \leq \delta_1 \leq \delta_2 \leq 2^{\lceil \frac{m}{2} \rceil} - 1$. Then there exists an AQC with the following parameters

$$[[n, n + m - m \left(\frac{\delta_1 + \delta_2}{2} \right), \{d_z, d_x\}]_2,$$

with $d_z = wt(B(\delta_2))$ and $d_x = wt(B(\delta_1))$.

Proof. The condition $\delta_i \leq 2^{\lceil \frac{m}{2} \rceil} - 1$ gives that the dimension of $B(\delta)$ is equal to $2^m - 1 - m \frac{\delta - 1}{2}$ from [26, Corollary 9.3.8]. We also have from [22, Lemma 1] that $B(\delta)^\perp \subset B(\delta)$. The minimum distance of $B(\delta_i)^\perp$ is larger than $2^{m-1} - 2^{\frac{m}{2}} \left(\frac{\delta_i - 1}{2} \right)$ by the Carlitz-Uchiyama bound [26, Theorem 9.9.18], and the Singleton bound gives that $wt(B(\delta_i)) \leq m \left(\frac{\delta_i - 1}{2} \right) + 1$. Hence the result follows from Lemma 2.2 by taking $C_1 = B^\perp(\delta_2)$ and $C_2 = B(\delta_1)$. \square

In Table 3, we compare the codes obtained using Lemma 2.7 and the construction in [1, Table 2], when using the same BCH codes.

Remark 2.8 By Lemma 2.7, we have the existence of AQC codes with parameters $[[511, 304, \{31, 17\}]]_2$ and $[[255, 183, \{15, 5\}]]_2$. From [1, Table 2, Table 3], we have the existence of AQC codes with parameters $[[1023, 70, \{32, 17\}]]_2$ and $[[255, 159, \{17, 5\}]]_2$ from BCH codes and LDPC codes. Table 3 shows that the construction provides codes with good rate gain.

Lemma 2.9 Let $n = 2^m - 1$, m odd, such that $\gcd(i, m) = 1$, where $2^i + 1 \leq 2^{\lceil \frac{m}{2} \rceil} - 1$. Furthermore, let B_i be the cyclic code with defining set $Cl(1) \cup Cl(2^i + 1)$, and $B(\delta_i)$ the BCH code with designed distance $\delta_i = 2^i + 1$. Then there exist AQC codes with parameters

$$[[2^m - 1, 2^m - 1 - m(2 + 2^{i-1}), \{d_{z_1}, 5\}]]_2, [[2^m - 1, m(2^{i-1} - 2), \{d_{z_2}, 5\}]]_2, \quad (1)$$

where $d_{z_1} = wt(B(\delta_i))$ and $d_{z_2} = wt(B(\delta_i)^\perp \setminus B_i^\perp)$.

When q is a prime power, there exists AQC codes with the following parameters

$$[[2q - 1, 2(k_1 - k_2), \{q - k_1, k_2 + 1\}]]_q.$$

Proof. The binary cyclic code B_i with defining set $Cl(1) \cup Cl(2^i + 1)$ (related to the Preparata codes), has parameters $[2^m - 1, 2^m - 2m - 1, 5]$, and $wt(B_i^\perp) = 2^{m-1} - 2^{\frac{m-1}{2}}$ from [7, Theorem 4.15]. Consider the binary BCH code $B(\delta_i)$ with $\delta_i = 2^i + 1 \leq 2^{\lceil \frac{m}{2} \rceil} - 1$. Hence the dimension of $B(\delta_i)$ is equal to $2^m - 1 - m2^{i-1}$. By the BCH bound, the minimum distance of $B(\delta_i)$ is at least $2^i + 1$. The Carlitz-Uchiyama bound gives that $wt(B_i \setminus B(\delta_i)^\perp) = 5$. By the Singleton bound we have $wt(B(\delta_i)) \leq m(2^{i-1}) + 1$, so that $wt(B(\delta_i) \setminus B_i^\perp) = wt(B(\delta_i))$. Then (1) follows from Lemma 2.2 by taking $C_2 = B_i$ and $C_1 = B(\delta_i)^\perp$ in the first case, and $C_2 = B_i$ and $C_1 = B(\delta_i)$ in the second case.

For the last part, consider two RS codes C_1 with parameters $[q - 1, k_1, q - k_1]_q$ and C_2 with parameters $[q - 1, k_2, q - k_2]_q$, such that $k_1 > k_2$. Extending C_i we obtain \overline{C}_i . Taking the direct sum $\mathcal{C}_i = C_i \oplus \overline{C}_i$ results in codes with parameters $[2q - 1, 2k_i, q - k_i]_q$. From the generator and parity check matrices, we can easily verify that $\mathcal{C}_i^\perp = C_i^\perp \oplus \overline{C}_i^\perp$. Hence by Lemma 2.2 we obtain an AQC with parameters $[[2q - 1, 2(k_1 - k_2), q - k_1/k_2 + 1]]_q$. \square

Example 2.10 There exist AQC codes from RS codes with the following parameters

$$[[31, 14, \{7, 3\}]]_{16}, [[31, 4, \{14, 2\}]]_{16} \text{ and } [[31, 22, \{4, 3\}]]_{16}.$$

2.2 Concatenated Construction

In [13], Ezerman et al. used the concatenated construction [26, Ch 10] for RS codes to obtain AQC codes over \mathbb{F}_4 with $d_x = 2$, so the emphasis was only on d_z . Thus their construction is limited in terms of the possible code parameters. Therefore, we first provide a modification of their construction.

Let q be a prime power and \mathbb{F}_{q^m} a finite extension of \mathbb{F}_q . The trace of an element α in \mathbb{F}_{q^m} is defined as $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = Tr_m(\alpha) = \sum_{i=0}^{m-1} \alpha^{q^i}$.

Two bases $B = \{\alpha_1, \alpha_2, \dots, \alpha_m\}$ and $B' = \{\beta_1, \beta_2, \dots, \beta_m\}$ of \mathbb{F}_{q^m} over \mathbb{F}_q are called dual bases if they satisfy

$$Tr_m(\alpha_i \beta_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

If a basis is the dual of itself, it is called a self-dual basis.

Let $B = \{\alpha_1, \alpha_2, \dots, \alpha_m\}$ be a basis of \mathbb{F}_{q^m} over \mathbb{F}_q . Then any $x \in \mathbb{F}_{q^m}$ can be written uniquely as $x = \sum_{i=1}^m a_i \alpha_i$, with $a_i \in \mathbb{F}_q$. Define the mapping

$$\Psi_B : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_q^m \quad (2)$$

$$x \mapsto \Psi_B(x) = (a_1, \dots, a_m). \quad (3)$$

This is an \mathbb{F}_q -linear mapping which is bijective and can be extended to

$$\Phi_B : \mathbb{F}_{q^m}^n \rightarrow \mathbb{F}_q^{mn} \quad (4)$$

$$(x_1, x_2, \dots, x_n) \mapsto (\Psi_B(x_1), \dots, \Psi_B(x_n)). \quad (5)$$

Lemma 2.11 *Let B be a basis of \mathbb{F}_{q^m} over \mathbb{F}_q and C an $[n, k, d]$ code over \mathbb{F}_{q^m} . Hence the code $\Phi_B(C) = \mathcal{C}$ is an $[nm, km, D \geq d]_q$ code. If C is an $[n, k, n - k + 1]_{q^m}$ MDS code, then there exists a code $\tilde{\mathcal{C}}$ over \mathbb{F}_q with parameters*

$$[(m+1)n, km, 2(n-k+1)]_q.$$

Proof. The first result is obvious, thus we prove only the second result. For this, let C be an $[n, k, n - k + 1]_{q^m}$ MDS code. Then $\Phi_B(C)$ is a code with parameters $[mn, mk, \geq d]_q$. This can be improved by adding an overall parity check to each element $\Psi_B(x)$ to obtain a q -ary code $\tilde{\mathcal{C}}$ with parameters $[(m+1)n, km, 2(n-k+1)]_q$ [26, Ch. 18.8]. \square

Lemma 2.12 *Let C be a linear code of length n over \mathbb{F}_{q^m} , and Φ the mapping defined in (4). In addition, let $B = \{\alpha_1, \dots, \alpha_m\}$ a basis of \mathbb{F}_{q^m} over \mathbb{F}_q , and $B^\perp = \{\beta_1, \beta_2, \dots, \beta_m\}$ its dual basis. Then we have $\Phi_{B^\perp}(C^\perp) = \Phi_B(C)^\perp$ and $\Phi_{B^\perp}(C^{\perp h}) = \Phi_B(C)^{\perp h}$.*

Proof. Assume that $c' = (y_1, \dots, y_n) \in C^\perp$. Hence $c \cdot c' = 0$ for all $c = (x_1, \dots, x_n) \in C$, where $x_i = \sum_{j=1}^m a_{ij} \alpha_j$ and $y_i = \sum_{j=1}^m b_{ij} \beta_j$. Then $c \cdot c' = \sum_{i=1}^n (\sum_{j=1}^m a_{ij} \alpha_j) (\sum_{j=1}^m b_{ij} \alpha_j) = 0$. The fact that $c \cdot c' = 0$ implies that $Tr_m(c \cdot c') = 0$, therefore

$$Tr_m \left(\sum_{i=1}^n \left(\sum_{j=1}^m a_{ij} \alpha_j \right) \left(\sum_{j=1}^m b_{ij} \beta_j \right) \right) = 0.$$

Applying the additivity property of the trace map, we obtain that this expression is equal to

$$\sum_{i=1}^n \text{Tr}_m \left(\left(\sum_{j=1}^m a_{ij} \alpha_j \right) \left(\sum_{j=1}^m b_{ij} \beta_j \right) \right) = 0.$$

From the additivity of the trace map and the duality of the basis, we have that

$$\text{Tr}_m(c \cdot c') = \sum_{i=1}^n \sum_{j=1}^m a_{ij} b_{ij} = 0. \quad (6)$$

Since

$$\Phi_B(c) = (\Psi_B(x_1), \dots, \Psi_B(x_n)) = (a_{11}, \dots, a_{1m}, a_{21}, \dots, a_{2m}, \dots, a_{n1}, \dots, a_{nm}),$$

and

$$\Phi_{B^\perp}(c') = (\Psi_{B^\perp}(y_1), \dots, \Psi_{B^\perp}(y_n)) = (b_{11}, \dots, b_{1m}, b_{21}, \dots, b_{2m}, \dots, b_{n1}, \dots, b_{nm}),$$

from (6) we obtain

$$\Phi_B(c) \cdot \Phi_{B^\perp}(c') = \sum_{i=1}^n \sum_{j=1}^m a_{ij} b_{ij} = 0.$$

Then $\Phi_{B^\perp}(C^\perp) \subset \Phi_B(C)^\perp$, and since both codes have the same dimension the result follows. The above proof also holds in the Hermitian case. \square

It is well known that the dual of an MDS code is also MDS. Thus if C_k is the RS code $[q^m - 1, k, n - k]_{q^m}$, its dual C_k^\perp is a $[q^m - 1, q^m - k, k + 1]_{q^m}$ code. Consider now the code $\Phi_{B^\perp}(C_k^\perp)$ which from Lemma 2.12 is equal to $\Phi_B(C_k)^\perp$. This is a code with parameters $[m(q^m - 1), m(q^m - k), \geq k + 1]_q$. Applying the construction of Lemma 2.11, we obtain that \mathcal{C}_k^\perp has parameters $[(m + 1)(q^m - 1), m(q^m - k), 2(k + 1)]_q$. Since Φ is a bijective map, if $k_1 > k_2$ then $\Phi_B(C_{k_2}) \subset \Phi_B(C_{k_1})$, and hence $\tilde{\mathcal{C}}_{k_2} \subset \tilde{\mathcal{C}}_{k_1}$. Applying Lemma 2.2, we obtain the following result.

Theorem 2.13 *Let q be an even prime power or q an odd prime and m odd. Then there exist AQC codes with parameters $[(m + 1)(q^m - 1), m(k_1 - k_2), \{2(q^m - k_1), 2(k_2 + 1)\}]_q$.*

In Table 4, we give some codes constructed from Theorem 2.13. Note that the codes of length 45 have better parameters than the codes given by Ezerman et al. [12, Table IX].

In a similar way as for classical codes, a concatenated quantum code [10] is constructed using two quantum codes, an outer code C and an inner code C' . If C is an $((n, K, d))_q$ code, then C' must be an $((n', K', d'))_K$ code, i.e., C' is a subspace of $\mathbb{C}^{K^{\otimes n'}}$. The concatenated code \mathcal{Q} is constructed as follows. For any codeword $|c\rangle = \sum_{i_1, \dots, i_{n'}} \alpha_{i_1, \dots, i_{n'}} |i_1, \dots, i_{n'}\rangle$ in C , replace each basis vector $|ij\rangle$, where $ij = 0, \dots, K - 1$ for $j = 1, \dots, n'$, with a basis vector $|x_{ij}\rangle$ in C' , i.e., $|c\rangle \mapsto |c'\rangle = \sum_{i_1, \dots, i_{n'}} \alpha_{i_1, \dots, i_{n'}} |x_{i_1}, \dots, x_{i_{n'}}\rangle$. Hence the resulting code \mathcal{Q} is an $((nn', K', D))_q$ code with $D \geq dd'$.

Table 4: Asymmetric quantum codes constructed from RS codes by Theorem 2.13

$[[45, 24, \{6, 4\}]]_4$	$[[45, 24, \{8, 2\}]]_4$	$[[45, 22, \{8, 4\}]]_4$
$[[45, 16, \{14, 4\}]]_4$	$[[45, 10, \{20, 4\}]]_4$	$[[45, 10, \{16, 8\}]]_4$
$[[186, 150, \{4, 2\}]]_2$	$[[186, 110, \{12, 10\}]]_2$	$[[186, 100, \{18, 6\}]]_2$
$[[186, 80, \{24, 10\}]]_2$	$[[186, 45, \{34, 16\}]]_2$	$[[186, 40, \{44, 6\}]]_2$

Theorem 2.14 *Let m be an integer, q a prime power, and m, k_1, k_2 and k positive integers less than or equal to $q^m - 3$. Then there exists a quantum code with parameters $[(m+1)(q^m-1)((q^m-2), m(k_1-k_2), \geq D)]_q$. $D = dd'$ where $d' = \min\{2(q^m - k_1), 2(k_2 + 1)\}$, $d = \min\{2(q^m - k - 1), k\}$.*

Proof. From [9, Proposition 4.2], we have the existence of AQMDS $[[q^m - 2, 1, \{q^m - k - 1, k\}]]_q$ codes for $k \leq q^m - 3$. Consider the concatenated code \mathcal{Q} with inner code the AQMDS $[[q^m - 2, 1, \{q^m - k - 1, k\}]]_q$ code. The outer code is the asymmetric quantum code given in Theorem 2.13. The above concatenation of quantum codes gives the result. \square

In the remainder of this section, we use the previous construction in the Hermitian case. We start by proving the following lemma. Assume that $q = p^2$ and that q is even or q and m are odd.

Lemma 2.15 *Let $q = p^2$ be an odd prime power such that $q \equiv 1 \pmod{4}$, n an even divisor of $q - 1$, and $s \leq n - 1$ an even integer. Then there exists an MDS negacyclic code C_s over \mathbb{F}_{q^2} of length n with defining set*

$$T_s = \{i \text{ odd} : 1 \leq i \leq s - 1\},$$

parameters $[n, n - \frac{s}{2}, \frac{s}{2} + 1]_{q^2}$ and which satisfies $C_s^{\perp h} \subset C_s$.

Proof. When $s = n - 1$, from [14, Theorem 16] we obtain that C_n is a negacyclic MDS code which is Hermitian self-dual. Assume now that $s \leq n - 1$ is an even integer and C_s is the negacyclic code with defining set $T_s = \{i \text{ odd} : 1 \leq i \leq s - 1\}$. Hence the BCH bound [4] gives that C_s has minimum distance $\frac{s}{2} + 1$. The dimension of C_s is $n - |T_s| = n - \frac{s}{2}$. This gives that C_s is an $[n, n - \frac{s}{2}, \frac{s}{2} + 1]_{q^2}$ code. The codes C and C_s are such that $C \subset C_s$, and hence $C_s^{\perp h} \subset C_n^{\perp h}$. The Hermitian dual $C_s^{\perp h}$ is a negacyclic MDS code with parameters $[n, \frac{s}{2}, n - \frac{s}{2} + 1]_{q^2}$. Since C_n is Hermitian self-dual, $C_s^{\perp h} \subset C_n \subset C_s$. \square

Assume now that we have a self-dual basis. Seroussi and Lempel [20] proved that \mathbb{F}_{q^m} has a self-dual basis over \mathbb{F}_q if and only if q is even or both q and m are odd. Consider the code $\Phi_{B^\perp}(C_s^{\perp h})$ which from Lemma 2.12 is equal to $\Phi_B(C_s)^{\perp h}$. This is a code with

parameters $[mn, m(n - \frac{s}{2}), \geq n - \frac{s}{2} + 1]$. Applying the construction of Lemma 2.11, we obtain that $C_s^{\perp h}$ has parameters $[(m+1)n, m(n - \frac{s}{2}), 2(n - \frac{s}{2} + 1)]_q$. Since Φ is a bijective map and $C_s^{\perp h} \subset C_s$, then $\Phi_B(C_s^{\perp h}) \subset \Phi_B(C_s)$, and hence $\tilde{C}_s^{\perp h} \subset \tilde{C}_s$. Applying Lemma 2.2, we obtain the following result.

Theorem 2.16 *Let $q = p^2$ be an even prime power or q an odd prime and m odd. Then there exist AQC's with parameters $[(m+1)n, m(n - s), \{2(\frac{s}{2} + 1), 2(n - \frac{s}{2} + 1)\}]_q$.*

References

- [1] S. A. Aly, A. Klappenecker and, P. K. Sarvepalli, *Remarkable degenerate quantum stabilizer codes derived from duadic codes*, in Proc. IEEE Int. Symp. Inform. Theory, Seattle WA, pp. 1105–1108, July 2006.
- [2] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, *On quantum and classical BCH codes*, IEEE Trans. Inform. Theory, 53(3), pp. 1183–1188, Mar. 2007.
- [3] A. Ashikhmin and E. Knill, *Non-binary quantum stabilizer codes*, IEEE Trans. Inform. Theory, 47(7), pp. 3065–3072, Nov. 2001.
- [4] N. Aydin, I. Siap and D. J. Ray-Chaudhuri, *The structure of 1-generator quasi-twisted codes and new linear codes*, Des. Codes Cryptogr. 24(3), pp. 313–326, 2001.
- [5] A. R. Calderbank, E. M. Rains, P. Shor, and N. J. A. Sloane, *Quantum error correction via codes over $GF(4)$* , IEEE. Trans. Inform. Theory, 44(4), pp. 1368–1387, July 1998.
- [6] A. R. Calderbank and P. W. Shor, *Good quantum error-correcting codes exist*, Phys. Rev. A 54(2), pp. 1098–1106, Aug. 1996.
- [7] P. Charpin, *Open problem on cyclic codes*, in V. S. Pless, W. C. Huffman, Eds., Handbook of Coding Theory, Vol. II, Elsevier, Amsterdam, pp. 1345–1439, 1998.
- [8] Z. W. E. Evans, A. M. Stephens, J. H. Cole, and L. C. L. Hollenberg, *Error correction optimisation in the presence of x/z asymmetry*, Available Online, arxiv.org/0709.3875/Sept. 2007.
- [9] Y. M. Chee, M. F. Ezerman, S. Jitman, H. M. Kia, and S. Ling, *Pure asymmetric quantum MDS codes from CSS construction*, <http://arxiv.org/abs/1006.1694>.
- [10] M. Grassl, P. Shor, G. Smith, J. Smolin, and B. Zeng, *Generalized concatenated quantum codes*, Phys. Rev. A, 79(5), 050306(R), 2009.
- [11] R. Lidl and H. Niederreiter *Finite Fields*, Encyclopedia of Mathematics and its Applications, Vol. 20, G. C. Rota, Ed., Cambridge Univ. Press: Cambridge, UK, 1983.

- [12] M. F. Ezerman, S. Ling, and P. Solé, *Additive asymmetric quantum codes*, IEEE. Trans. Inform. Theory, 57(8), pp. 5536–5550, Aug. 2011.
- [13] M. F. Ezerman, S. Ling, P. Solé, and O. Yemen, *From skew-cyclic codes to asymmetric quantum codes*, Adv. Math. Commun., 5(1) pp. 41–57, 2011.
- [14] K. Guenda, *New MDS self-dual codes over finite fields*, Des. Codes Cryptogr., 62(11), pp. 31–42, Jan. 2012.
- [15] M. Grassl, T. Beth, and M. Rotteler, *On optimal quantum codes*, Int. J Quantum Inform., 2(2), pp. 55–64, 2004.
- [16] W. C. Huffman and V. S. Pless, *Fundamentals of Error-correcting Codes*, Cambridge University Press: Cambridge, UK, 2003.
- [17] L. Ioffe and M. Mézard, *Asymmetric quantum error-correcting codes*, Phy. Rev. A, 75, 032345, 2007.
- [18] L. Jin, S. Ling, J. Luo, and C. Xing, *Application of classical hermitian self-orthogonal MDS codes to quantum MDS codes*, IEEE. Trans. Inform. Theory, 56(9), pp. 4735–4740, Sept. 2010.
- [19] P. K. Sarvepalli, A. Klappenecker, and M. Rotteler, *Asymmetric quantum codes: Constructions, bounds and performance*, Proc. R. Soc. A, 465, pp. 1645–1672, 2009.
- [20] G. Seroussi and A. Lempel, *Factorization of symmetric matrices and trace-orthogonal bases in finite fields*, SIAM, J. Computing, 9, pp. 758–767, 1980.
- [21] P. W. Shor, *Scheme for reducing decoherence in quantum memory*, Phy. Rev. A, 52(4), pp. 2493–2493, 1995.
- [22] A. M. Steane, *Enlargement of Calderbank-Shor-Steane quantum codes*, IEEE. Trans. Inform. Theory, 45(7), pp. 2492–2495, Nov. 1999.
- [23] A. Steane, *Multiple particle interference and quantum error correction*, Proc. Royal Soc. London A, 452(1954), pp. 2551–2577, Nov. 1996.
- [24] A. M. Steane, *Error correcting codes in quantum theory*, Phys. Rev. Lett., 77(5), pp. 793–797, July 1996.
- [25] P. Steane, *Simple quantum error-correction codes*, Phys. Rev. A, 54(6), pp. 4741–4751, Dec. 1996.
- [26] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland: Amsterdam, 1977.

- [27] L. Wang, K. Feng, S. Ling, and C. Xing, *Asymmetric quantum code: Characterization and constructions*, IEEE. Trans. Inform. Theory, 56(11), pp. 2938–2945, Nov. 2010.
- [28] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, MIT Press: Cambridge, MA, 1972.